ASSIGNMENT 4

Textbook Assignment: "AIS Security (continued)," chapter 4, pages 4-13 through 4-26.

4-1. In which of the following steps in planning an AIS security program, will major problem areas be identified?

1. Perform action plans
2. Perform preliminary planning
3. Perform a preliminary risk analysis
4. Perform and document a detailed risk analysis

4-2. Which of the following steps in planning an AIS security program allows for review and approval?

1. Perform action plans
2. Perform preliminary planning
3. Perform a preliminary risk analysis
4. Perform and document a detailed risk analysis

4-3. A security policy statement should provide which of the following information?

1. General guidance and assignment of responsibilities
2. General guidance and listing of responsibilities
3. Detailed guidance and assignment of responsibilities
4. Detailed guidance and listing of responsibilities

4-4. As a guideline for risk analysis, which of the following FIPS publications should you use?

1. FIPS PUB 47
2. FIPS PUB 53
3. FIPS PUB 65
4. FIPS PUB 79

4-5. The impact of a given threat may depend on all but which of the following factors?

1. Geographical location
2. Local environment
3. Perceived threat of vandals
4. Potential value of property to a thief

4-6. Which of the following is a threat to an AIS facility?

1. Hardware failure
2. Tampering with inputs, programs, and data
3. Accidents causing nonavailability of key personnel
4. Each of the above

4-7. It is recommended that the AIS facility upper management begin development of the security program with a/an

1. risk analysis
2. inventory of equipment
3. survey of data integrity
4. intensive training program

4-8. A quantitative risk analysis produces which of the following results?

1. Long-range planners receiving guidance on personnel requirements
2. The security program objectives directly relating to the mission of the command
3. Criteria generated for designing and evaluating internal controls
4. An estimate of losses to be expected

4-9. When the risk analysis is prepared, the first step to be considered is to

1. develop an estimate of annual loss expectancy
2. estimate the potential losses to which the AIS facility is exposed
3. evaluate the threats to the AIS facility
4. review the security program objectives

4-10. The loss potential estimate has which of the following objectives?

1. To place a monetary value on the loss estimate only
2. To identify critical aspects of the AIS facility operation only
3. To place a monetary value on the loss estimate and to identify critical aspects of the AIS facility operation
4. To determine data replacement requirements

4-11. The loss of program files has which of the following loss potentials?

1. Cost to replace assets
2. Cost to reconstruct files
3. Security compromise
4. Value of assets stolen before loss is detected

4-12. Which of the following is the loss potential that may result from the indirect theft of assets?

1. Cost to replace assets
2. Cost to reconstruct files
3. Security compromise
4. Value of assets stolen before loss is detected

4-13. To show replacement costs for the physical assets of the AIS facility, AIS technical managers and upper management should use which of the following methods?

1. Build a graph
2. Construct a table
3. Produce a list
4. Write a description

4-14. The AIS technical manager should call on which of the fallowing personnel to assist in making loss estimates?

1. Users
2. Vendors
3. Programmers
4. Supervisors

4-15. After a preliminary screening to identify the critical tasks, the AIS technical manager should perform which of the following tasks next?

1. Determine the scope of the critical tasks
2. Develop an estimate of annual loss expectancy
3. Quantify loss potential with the help of user representatives
4. Determine the back-up system requirements for the critical tasks

4-16. The second step to be considered when you prepare the risk analysis is to

1. develop an estimate of annual loss expectancy
2. estimate the potential losses to which the AIS facility is exposed
3. evaluate the threats to the AIS facility
4. review the security program objectives

4-17. To develop estimates of the occurrence probability for each type of threat, the AIS technical manager should use all except which of the following resources?

1. Standardized Navy-wide formula
2. Higher authority instructions/manuals
3. Common sense
4. Data

4-18. The third step to be considered when you prepare the risk analysis is to

1. develop an estimate of annual loss expectancy
2. estimate the potential losses to which the AIS facility is exposed
3. evaluate the threats to the AIS facility
4. review the security program objectives

4-19. Fire, flood, and sabotage, in varying degrees, result in which of the following losses?

1. Indirect loss of assets
2. Physical destruction
3. Data compromise
4. Theft of information

4-20. Reducing the probability of some occurrence by altering the environment could be accomplished in which of the following ways?

1. Implementing more rigorous standards for programming and software testing
2. Preparing a backup system for offsite operations
3. Providing military guards and special door locks
4. Relocating the AIS facility

4-21 Which of the following is an example of erecting barriers to ward off a threat?

1. Implementing more rigorous standards for programming and software testing
2. Preparing a backup system for offsite operations
3. Providing military guards and special door locks
4. Relocating the AIS facility

4-22. When selecting a specific remedial measure, a total of how many criteria should be used?

1. One
2. Two
3. Three
4. Four

4-23. Which of the following is one possible way to select a remedial measure to minimize a threat?

1. Begin with the threat having the largest annual loss potential
2. Begin with only those measures for which the cost can be estimated precisely
3. Begin with only those remedial measures that would not cause a loss reduction in the same area
4. Begin with the remedial measures for which the annual cost is more than the expected reduction in annual loss

4-24. All but which of the following events tends to have the same basic effect as the others on AIS operations?

1. Fire
2. Rain
3. Earthquake
4. Windstorm

4-25. In minimizing an AIS building's exposure to fire damage, which of the following factors should be considered?

1. Contractors
2. Design only
3. Location only
4. Design and location

4-26. An AIS physical security program should include which of the following fire safety elements?

1. Measures to ensure prompt detection of and response to a fire emergency
2. Provision for quick human intervention and adequate means to extinguish fires
3. Provision of adequate means and personnel to limit damage and effect prompt recovery
4. All of the above

4-27. In evaluating the fire safety of an AIS facility, a total of how many factors are to be considered?

1. Five
2. Six
3. Three
4. Four

4-28. Which of the following factors affects the degree of hazard associated with a given occupancy?

1. Weight of the material
2. Amount of combustible material
3. Exposed surface of the material
4. Package in which the material is stored

4-29. When the safety features of an AIS facility building are designed, which of the following factors should be considered?

1. Heat-resistant lights
2. Building operation
3. Fire walls
4. Storm doors

4-30. The inherent fire safety of a building can be rendered ineffective because of which of the following conditions?

1. Fire doors propped open
2. Standard electrical wiring
3. Use of low-flame spread materials
4. Products-of-combustion detectors

4-31. Experience in fire fighting shows that the major factor in limiting fire damage is

1. prompt detection of fires
2. experienced fire fighters
3. multiple fire extinguishers
4. quick response time to alarms

4-32. During the third stage of a fire, fire fighting becomes increasingly difficult and often people cannot remain at the fire site for which of the following reasons?

1. Toxic gases only
2. High temperatures only
3. Large volume of smoke only
4. Toxic gases, high temperatures, and large volume of smoke

4-33. Prompt fire detection is best accomplished through the use of which of the following detectors?

1. Gas
2. Heat
3. Smoke
4. Flame

4-34. When detectors are installed, which of the following factors need NOT be considered?

1. The location of equipment
2. The direction and velocity of air flow
3. The presence of areas with stagnant air
4. The location of fire extinguishers

4-35. In the design of the detection control panel, which of the following indications should be included?

1. The power supply status of each detector
2. Which detector has alarmed
3. The cause of the alarm
4. What type of detector has alarmed

4-36. To assure that someone will be alerted to a fire, which of the following alarm locations is recommended as the primary location?

1. Computer room
2. Personnel office
3. Commanding officer's office
4. Buildinq maintenance

4-37. Reducing the sensitivity of the smoke detectors to eliminate nuisance alarms may have which of the following results?

1. Save energy
2. Extend equipment life
3. Delay fire detection
4. Cause poor personnel performance

4-38. In an actual fire situation, the air handling equipment could be shut down automatically to avoid which of the following problems?

1. Straining the air handling equipment
2. Excessive energy consumption
3. Excessive filter wear
4. Spreading smoke and fanning the flames

4-39. When fire detection systems are interconnected with air handling equipment, a preferred technique is to cause the system to take which of the following measures?

1. Exhaust the smoke
2. Lower the thermostat
3. Recirculate the smoke
4. Use inside air for intake

4-40. What is the minimum temperature required to activate an automatic sprinkler system?

1. 115°F
2. 125°F
3. 135°F
4. 145°F

4-41. To ensure the effectiveness of portable extinguishers, which of the following measures should be observed?

1. Extinguishers should be marked for rapid identification
2. Extinguishers should have inspection tags
3. Extinguishers should be placed in corners
4. Extinguishers should be placed on the floor, not mounted

4-42. Military personnel who are knowledgeable and trained in fire safety are needed by which of the following types of commands?

1. Small commands only
2. Medium commands only
3. Large commands only
4. Every command

4-43. When using supporting utilities, AIS technical managers should consider the probability of occurrence and the effects of which of the following conditions?

1. Vandalism only
2. Sabotage only
3. Fire only
4. Vandalism, sabotage, and fire

4-44. Excessive fluctuation in the dc voltage applied to the hardware can be caused if the line voltage is 90 percent or less of nominal for more than what minimum number of milliseconds?

1. 7
2. 6
3. 5
4. 4

4-45. Power fluctuations in line voltage cause unpredictable results in which of the following components?

1. Logic only
2. Hardware only
3. Data transfer only
4. Logic, hardware, and data transfer

4-46. In an AIS facility, the effects of internal power fluctuations can be minimized in which of the following ways?

1. Grounding the CPU
2. Isolating the AIS hardware from other facility loads
3. Wiring all components in parallel
4. Wiring each component with a circuit breaker

4-47. The technique of connecting the AIS facility to more than one utility feeder has more protection value when the feeders are connected in what manner?

1. To the same junction box
2. From the same utility pole
3. To different power substations
4. To different utility meters

4-48. An uninterrupted power supply (UPS) consists of a solid-state rectifier that performs which of the following functions?

1. Drives a solid-state inverter only
2. Keeps batteries charged only
3. Drives a solid-state inverter and keeps batteries charged
4. Synthesizes alternating current

4-49. The UPS battery supply can support a facility load for a maximum of how many minutes?

1. 35
2. 40
3. 45
4. 50

4-50. The control circuitry for a static transfer switch performs which of the following functions?

1. Senses variations in frequency
2. Senses an overcurrent condition
3. Switches the load to the alternate power source
4. Stops the flow of power

4-51. Using multiple, independent UPS units can provide which of the following benefits?

1. Power consumption is lowered
2. Each unit can be switched offline if it fails
3. The metering of component power consumption is facilitated
4. All of the above

4-52. If the risk analysis shows a major loss from power outages lasting 30 to 45 minutes or longer, which of the following measures should be taken?

1. Installing an on-site generator
2. Cutting back on operations
3. Relocating the facility
4. Adding more multiple, independent UPS units

4-53. Which of the following components must be large enough to support air-conditioning or minimum lighting as well as the UPS load?

1. Generator
2. Alternator
3. Prime mover
4. Alternate mover

4-54. Providing physical protection for an AIS facility involves which of the following processes?

1. Denying access to unauthorized persons
2. Permitting access to authorized persons
3. Both 1 and 2 above
4. Minimizing the risks of a natural disaster

4-55. Wherever AIS equipment is used for processing classified information, which of the following instructions should be used for applying physical protection and security policy?

1. OPNAVINST 5230.12
2. OPNAVINST 5239.1
3. SECNAVINST 5211.5
4. SECNAVINST 5233.1

4-56. Which of the following contingency plans for dealing with classified material should NOT be considered in emergencies?

1. Destruction
2. Protection
3. Removal
4. Reproduction

4-57. In an emergency, the placement of a perimeter guard force around the affected area provides protection in which of the following ways?

1. Provides external contact when communications are lost
2. Prevents the removal of classified material
3. Reduces the risk of additional destruction
4. Provides AIS access control

4-58. Which of the following methods may be used to protect the property boundary of the AIS facility?

1. Roving patrol only
2. Fencing-only
3. Roving patrol and fencing
4. Security badges

4-59. Fences installed for boundary protection should be (a) what minimum height with (b) what minimum number of strands of barbed wire?

1. (a) 8 feet (b) 2
2. (a) 8 feet (b) 3
3. (a) 10 feet (b) 2
4. (a) 10 feet (b) 3

4-60. Penetration sensors mounted on fences and gates should provide which of the following alarms when tripped?

1. External only
2. Internal only
3. External and internal

4-61. Tests show that electromagnetic or acoustic emanations from AIS hardware. may be intercepted up to a maximum of how many yards away?

1. 150
2. 230
3. 325
4. 400

4-62. If the AIS technical manager plans to take measures to control compromising emanations, those measures are subject to approval under the provisions of which of the following DOD directives?

1. 5200.19
2. C5200.19
3. 5200.28
4. C5200.28

4-63. The application of the measures to control compromising emanations within the industrial AIS systems is at the direction of the contracting activity concerned under the provisions of which of the following DOD directives?

1. 5200.19
2. C5200.19
3. 5200.28
4. C5200.28

4-64. The use of an intrusion detection system (IDS) in a protective program is covered in which of the following instructions?

1. OPNAVINST 5239.1
2. OPNAVINST 5510.1
3. SECNAVINST 5211.5
4. SECNAVINST 5233.1

4-65. The physical security requirements for a remote terminal area are based upon which of the following classifications?

1. The classification of the central computer facility
2. The classification of the remote terminal area
3. The classification of the data that will be accessed through the terminal
4. The classification assigned by higher authority

4-66. When the AIS system contains classified information, what action, if any, must be taken for each remote terminal that is not controlled?

1. Disconnect
2. Place offline
3. Turn off
4. None

4-67. In the annual security survey of an AIS facility, what is the second step?

1. Define and tabulate areas within the facility for control purposes
2. Evaluate all potential threats to the AIS facility
3. Identify areas where remedial measures are needed
4. Recommend improvements to upper management

4-68. When the annual security survey is conducted, it should begin at which of the following areas?

1. Roof
2. Basement
3. Perimeter
4. Top floor

4-69. When surveying the perimeter of the facility, the AIS technical manager need NOT check which of the following accessways?

1. Fire escapes
2. Doors and windows
3. Other entrances, such as vents
4. Manned posts at the property line

4-70. When surveying the internal security of a facility, the AIS technical manager should follow which of the following guidelines?

1. Begin the survey on the roof
2. Determine where alarms annunciate
3. Finish the survey in the mailroom area
4. Note the volume of the alarms

IN ANSWERING QUESTION 4-71, REFER TO TABLE 4-6 IN THE TEXT.

4-71. Which of the following questions need NOT be included in the physical security survey?

1. Is the present equipment up-to-date?
2. Is the alarm system inspected and tested occasionally to ensure operation?
3. What kind of sound does the alarm make?
4. How many zones of protection are within the protected building?

4-72. Which of the following facts are used by the AIS technical manager to evaluate existing access controls and protection measures?

1. The schedule of alarm tests
2. The design of the alarm system
3. The number and location of manned posts
4. The distance between the manned posts and the building

4-73. Which of the following items are prepared and executed for the accomplishment of the command’s specific mission?

1. Operation plans only
2. Operation plans and-the command’s organizational manual
3. Emergency response plans only
4. Emergency response plans and the command’s organizational manual

4-74. A total of how many different types of contingency plans make up a COOP security plan?

1. One
2. Two
3. Three
4. Four

4-75. The risk analysis should be reviewed by which of the following people?

1. Production control clerk
2. Response team
3. Technical manager
4. Upper management